

УДК 004.056.53

Нагорна Н.М.¹

¹ старш. викл. НУ «Запорізька політехніка»

ЗАХИСТ НАДВЕЛИКИХ ІНТЕГРОВаних СХЕМ І СИСТЕМ НА КРИСТАЛІ ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

Життєвий цикл мікросхеми включає етапи проектування та експлуатації. Вже на першому етапі проектування при формуванні технічного завдання, необхідно позначити вимоги до заходів захисту мікросхеми від непередбачених впливів і визначити рівень безпеки.

Способи захисту можуть бути програмними та апаратними. Апаратні способи дозволяють:

- захистити кристал мікросхеми від механічних впливів при проведенні реінжинірингу;
- захистити блоки пам'яті за допомогою створення блоку керування правами доступу до пам'яті;
- захистити кристал від перевищення номінальних значень електричних параметрів.

Сучасні пристрої типу надвеликих інтегрованих схем (НВІС) і систем на кристалі (СнК) мають захищену інформацію щодо проєкту (ІР-захист) і захищені дані. Такий захист можливий завдяки:

можливості знищення всіх критичних даних у момент несанкціонованого втручання;

завантаженню ключа шифрування користувача за допомогою секретного ключа, вбудованого в мікросхему при її виробництві;

IP-захисту, який не дозволяє вносити зміни до проєкту і контролює можливість копіювання проєкту.

Наприклад, СнК, реалізовані за технологією SmartFusion2 корпорації Microsemi, мають вбудовані блоки, які виконують наступні функції захисту даних:

- блок недетермінованого генератора випадкових двійкових послідовностей (NRBG);

- блок криптографічного сервісу користувача з виконанням шифрування за стандартами AES 128 / -256, SHA 256 та HMAC;

- апаратні засоби мережевого захисту (firewalls) доступу до пам'яті мікроконтролерної підсистеми.

Визначною особливістю СНК SmartFusion2, яка дозволяє мати IP-захист і захист даних, є наявність енергонезалежної програмованої логічної матриці, виконаної за флеш-технологією.

У вказаній матриці конфігураційна flash пам'ять рівномірно розподілена площею кристала. Для її роботи не потрібна мікросхема зовнішньої конфігураційної пам'яті, тому не потрібно і завантажувати конфігурацію з неї. Програмована логічна матриця готова до роботи практично відразу після включення.

Крім того, під час конфігурування матриці неможливо підключитися до потоку конфігураційних даних та зчитати його без санкції на зчитування.

На етапі функціонально-логічного проєктування НВІС та СнК для захисту пристроїв використовуються методи обфускації у якості апаратного захисту.

В методах обфускації змінюється логічна структура мікросхеми за рахунок додавання до неї додаткових логічних елементів і ключових входів. Вказаний процес називається логічним кодуванням. Він дозволяє змінювати комбінаційну частину функціональних блоків. Функціональний блок працює за заданим алгоритмом, якщо на його ключові входи надходять сигнали у відповідності з секретним ключем, що зберігається у вбудованій пам'яті (рис. 1).

У цьому разі зловмиснику, який не має ключа, недоступна внутрішня структура пристрою.

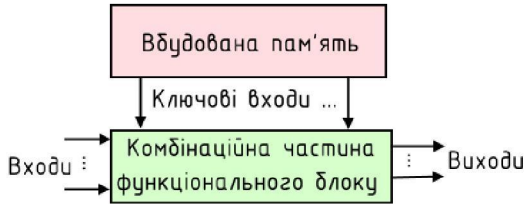
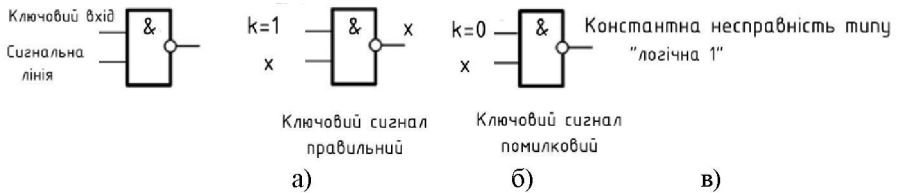


Рисунок1 – Змінення структури функціонального блоку при логічному кодуванні

На рис. 2 на прикладі логічного елемента 2І-НЕ проілюстрований принцип обфускації.



- а) – логічний елемент І-НЕ має додатковий ключовий вхід;
 б) – робота ЛЕ І-НЕ при справжньому ключі;
 в) – робота ЛЕ І-НЕ при несправжньому ключі

Рисунок 2 – Ілюстрація методу логічного кодування